Internet voting *not* impossible

Wolter Pieters (Nijmegen, Netherlands)
Joe Kiniry (Dublin, Ireland)

November 16, 2004

In the Communications of the ACM of October 2004, an evaluation was presented of the SERVE Internet voting system developed in the USA (Jefferson, Rubin, Simons and Wagner, "Analyzing Internet Voting Security", CACM 47(10):59-64). This paper is very critical towards Internet voting, and seems to advise not to use this technology at all, because of inherent vulnerabilities. However, in the Netherlands, we do have positive experience with online voting, and we wish to point to feasible alternatives in order to give a more balanced picture of the field.

Two main arguments against Internet voting can be distinguished in the aforementioned paper. Firstly, it is argued that the system allows for vote buying and selling. However, this holds for any voting system in which voters vote at home. Internet voting can only be fairly compared to postal ballots, not to voting at polling stations. If we want to do home voting, measures can be taken (technical, organisational, and legal) that make it unattractive to buy or sell votes.

A second argument against Internet voting is that the technology is vulnerable to attacks. Although we recognize that the Internet is a hostile environment, a system called RIES, developed for elections for public water management authorities in the Netherlands, has two main features which give us confidence in the limited possibilities of attacking the system.

First of all, a reference table is published before the elections, including (anonymously) for each voter the hashes of all possible votes, linking those to the candidates. It is possible to compare the number of voters in this table with the number of registered voters.

After the elections — and this is the second feature — a document with all received votes is published. This allows for two important verifications: a voter can verify his/her own vote, including the correspondence to the chosen candidate, and anyone can do an independent calculation of the result of the elections, based on this document and the reference table published before the elections. If your vote has been registered wrongly, or not at all, you can detect it. And if the result is incorrect given the received votes, you can detect it as well.

The main technical trick that achieves all this is the clever use of hash functions. Whereas the hashes of all possible votes are public, it is impossible to deduce valid votes from them without the required voter key. Of course, the relation between voter and voter key should not be stored anywhere, but the same holds for bank access codes. Procedures that achieve this therefore already exist.

The RIES system has been developed by the public water management authority of Rijnland and Mullpon v.o.f., and will be patented. The system has worked well in an actual election with 70,000 voters. Although Internet voting should not be the only way of voting offered in an election (due to accessibility issues and possible denial-of-service attacks), we think that Internet voting is feasible, as long as we do not require it to be *more* secure than present systems.